ENKRIPSI DAN DEKRIPSI PADA MESIN ENIGMA

Augried Leoni Famela[1)], Loeky Haryanto[2)], Armin Lawi[3)]
augried283@gmail.com[1)], L.Haryanto@unhas.ac.id[2)], armin.lawi@gmail.com[3)]
[1]Jurusan Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam,Universitas Hasanuddin
Jln. Perintis Kemerdekaan, Makassar, Indonesia, Kode Pos 90245

ENCRYPTION AND DECRYPTION OF ENIGMA MACHINE

Augried Leoni Famela[1)], Loeky Haryanto[2)], Armin Lawi[3)]
augried283@gmail.com[1)], L.Haryanto@unhas.ac.id[2)], armin.lawi@gmail.com[3)]
[1]Departement of Mathematic, Faculty of Mathematics and Natural Sciences, Hasanuddin University
Perintis Kemerdekaan Street, Makassar, Indonesia, Post Code 90245

ABSTRAK

Proses enkripsi maupun dekripsi suatu pesan pada mesin Enigma sesungguhnya adalah proses substitusi setiap huruf di dalam pesan menjadi huruf yang berbeda dan sebagai akibatnya, sebuah huruf yang muncul dua kali dalam pesan tersebut cenderung disubstitusi menjadi dua huruf yang berbeda. Dengan menggunakan mesin Enigma M3, proses substitusi pada mesin terjadi pada tiga komponen utama Enigma: *plugboard*, (tiga buah) *rotor* dan *reflector*. Karena proses substitusi huruf melalui *plugboard* dan ketiga *rotor* terjadi dua kali, proses enkripsi (dan dekripsi) terdiri atas lima langkah substitusi utama berikut.

Dengan menggunakan konsep permutasi, proses enkripsi (dan dekripsi) terhadap sebuah huruf diawali oleh substitusi dengan menggunakan plugboard dan substitusi ini bersesuaian dengan suatu permutasi γ: $\mathbf{Z}_{26}\rightarrow\mathbf{Z}_{26}$. Berdasarkan sifat dari plugboard, berlaku $\gamma^2 = 1$ (permutasi identitas). Langkah kedua adalah tiga kali substitusi oleh tiga *rotor*, masing-masing bersesuaian dengan tiga permutasi δ, μ dan τ. Langkah berikutnya adalah substitusi oleh *reflector* yang bersesuaian dengan suatu permutasi η yang memenuhi sifat $\eta^2 = 1$. Dua langkah utama terakhir adalah dua kelompok subtitusi yang bersesuaian dengan permutasi-permutasi τ^{-1}, μ^{-1}, δ^{-1}(oleh tiga rotor) dan permutasi γ^{-1} (oleh plugboard) sehingga secara keseluruhan, sebuah huruf di dalam pesan dienkripsi melalui subsitusi yang bersesuaian dengan hasil kali permutasi $\gamma\delta\mu\tau\eta\tau^{-1}\mu^{-1}\delta^{-1}$. Karena $(\gamma\delta\mu\tau\eta\tau^{-1}\mu^{-1}\delta^{-1}\gamma^{-1})(\gamma\delta\mu\tau\eta\tau^{-1}\mu^{-1}\delta^{-1}) = 1$, proses dekripsi terhadap huruf sandi yang diperoleh bisa dikerjakan dengan menggunakan mesin yang sama dan dengan kunci (rahasia) yang sama.

Penelitian literatur ini dikerjakan untuk mendapatkan hasil-hasil perhitungan secara kombinatorik semua kemungkinan dari setiap permutasi yang bersesuaian dengan substitusi-substitusi dalam proses enkripsi (dan dekripsi) oleh mesin Enigma M3, seperti yang diuraikan di atas.

Kata kunci : Enigma, mesin kripto, mesin enigma, rotor, plugboard,reflektor

ABSTRACT

The encrypting and decrypting processes of a message by an Enigma machine are actually*substituting processes* of a characterin the message by another (different) character and therefore, a character appearing twice in the message will be likely to be substituted with two different characters. Using Enigma M3 machine, the *substitution* process in the Enigma machine occurs in each of the the three main components of Enigma: a plugboard, (three) rotors and a reflector. Since the substitution process by each plugboard and rotors occur twice respectively, the overall substitution processes consists of the following five primary steps.

Using the notion of permutation, the encription (and decription) process on a letter starts with the plugboard substituting the letter with another letter and this substitution process corresponds to a permutation γ: $\mathbf{Z}_{26}\rightarrow\mathbf{Z}_{26}$. Based on the nature of the plugboard, the equality $\gamma^2 = 1$ (identity permutation) holds. The second primary step is three subtitions caused by the moves of three rotors, each substitution corresponds to permutation δ, μ dan τ. The next primary step is a substitution by reflector that corresponds to a prmutation η satisfying $\eta^2 = 1$. The last two primary steps correspond to τ^{-1}, μ^{-1}, δ^{-1}

permutations (by three rotors) and the permutation γ^{-1} (by plugboard) so overall, a letter in the message is encrypted by a series of permutations corresponding to a product of permutations $\gamma\delta\mu\tau\eta\tau^{-1}\mu^{-1}\delta^{-1}$. Since the equality $(\gamma\delta\mu\tau\eta\tau^{-1}\mu^{-1}\delta^{-1}\gamma^{-1})(\gamma\delta\mu\tau\eta\tau^{-1}\mu^{-1}\delta^{-1}) = 1$ holds, the decryption process of the encrypted letter using the Enigma M3 machine can be done using the same machine and the same (secret) keys.

This literature study is conducted to obtain the total number of all possibilities for each possible permutations corresponding to substitutions used in the encryption (or decryption) in the Enigma machine M3, as described above.

Keywords : Enigma, crypto machine, enigma machine, rotor, reflector, plugboard

I. Pendahuluan

Mesin Enigma merupakan mesin kripto berbasis rotor yang digunakan untuk mengenkripsi dan mendekripsi pesan rahasia. Mesin Enigma dipatenkan oleh seorang insinyur asal Jerman yang bernama Arthur Scherbius pada tahun 1918, yang kemudian digunakan oleh militer dan pemerintah Jerman Nazi sebelum dan selama Perang Dunia II. Pada awalnya Nazi menganggap bahwa Enigma adalah mesin kriptografi teraman di dunia. Namun pihak sekutu terus berusaha keras untuk memecahkan kode *cipher* yang dihasilkan oleh Enigma. Mesin Enigma terdiri atas 7 komponen utama, yaitu *plugboard*, rotor, penggerak rotor, reflektor, *keyboard, lampboard* dan kotak Enigma. Enkripsi yang dilakukan Enigma sebenarnya adalah substitusi (bijeksi), di mana sebuah huruf digantikan dengan tepat sebuah huruf juga, hanya saja substitusi dilakukan beberapa kali. Dan walau hanya dengan substitusi, sebuah pesan akan sulit sekali didekripsi jika tidak dengan alat yang sama, dengan pengaturan posisi yang sama, tipe substitusi yang sama, dan kode kunci yang sama.

II. Komponen Enkripsi dan Dekripsi Enigma

Komponen utama Enigma yang berperan dalam enkripsi /dekripsi pesan adalah keyboard, plugboard, rotor, reflektor, papan lampu.

II.a Keyboard

Keyboard memiliki tata letak QWERTZUI , tanpa nomor , spasi atau tombol lainnya . Menekan sebuah tombol akan membuka sinyal dari huruf yang ditekan dan secara mekanis dilanjutkan ke rotor 1 sampai rotor 3.

II.b Plugboard

Plugboard di Enigma ini terdiri dari satu Panel listrik yang berisis 26 huruf alphabet beserta colokan di masing-masing huruf tersebut. *Plugboard* atau Panel steker digunakan untuk menukar 2 buah huruf. Karena terdapat 26 huruf maka secara teoritis

maksimum kabel yang dibutuhkan sebanyak 13 kabel. Untuk tiap jumlah kabel yang digunakan dimulai dari tanpa nomor sampai dengan nomor 13.

II.c Rotor

Sebuah rotor merupakan sebuah piringan yang terbuat dari karet yang keras atau bakelit dengan deretan kuningan yang berisi pin-pin yang menonjol yang berbentuk bundar. Di sisi satunya bersesuaian dengan deretan angka yang juga berbentuk bundar. Untuk menghindari *cipher* substitusi sederhana, beberapa rotor harus diputar berdasarkan penekanan sebuah kunci. Alat yang paling banyak digunakan untuk mengimplementasikan pergerakan rotor tersebut adalah mekanisme rotor bergigi dan sebuah penggerak rotor tersebut. Penggerak rotor tersebut memutar rotor sebanyak satu karakater ketika sebuah huruf diketikkan pada *keyboard*.

II.d Reflektor

Komponen ini, selain digunakan untuk memastikan bahwa sebuah huruf tidak dikodekan terhadap dirinya sendiri, juga berguna untuk menjadikan mesin ini bersifat *reversible*, maksudnya apabila sebuah huruf dienkripsikan kembali, maka hasil enkripsi huruf tersebut adalah huruf semula. Reflektor memiliki 26 kontak seperti rotor tetapi hanya satu himpunan alphabet. Setiap huruf terhubung ke huruf lainnya dengan kawat (pada dasarnya menukar huruf seperti plugboard). Pada reflektor, pertukaran pada 26 huruf tidak pernah berubah.

II.e Papan Lampu

Panel Lampu mengikuti tata letak yang sama seperti *Keyboard* dan *Plugboard* . Setiap huruf memiliki bola lampu di bawahnya, yang menyala untuk menunjukkan huruf itu dienkripsi atau diuraikan , yang kemudian harus ditulis

III. Cara Kerja Mesin Enigma

Mesin Enigma bekerja berdasarkan perputaran rotor-rotor yang ada di dalamnya. Ketika sebuah huruf diketikkan pada *keyboard*, arus listrik akan mengalir pada mesin ini yang diawali melewati *plugboard*, kemudian terus melewati 3 rotor dan setelah tiba di reflektor arus listrik dibalikkan kembali melewati 3 rotor selanjutnya diteruskan ke *plugboard* dan kemudian huruf yang dienkripsi ditampilkan pada lampu yang menyala. Setelah tampilan huruf yang telah dienkripsi menyala, rotor berputar. Perputaran rotor sama halnya dengan sebuah Odometer yaitu jika rotor yang paling kanan telah menyelesaikan satu putaran penuh, rotor yang ditengah berubah satu posisi dan begitu seterusnya untuk rotor yang berikutnya. Ketika arus melewati tiap komponen yang ada di dalam mesin Enigma ,

huruf mengalami pemetaan ke dalam huruf yang lain. *Plugboard* melakukan pemetaan yang pertama. Jika terdapat sambungan antara dua huruf, huruf-huruf ini akan dipertukarkan satu sama lain. Misalnya jika sambungan A dan F, maka F akan dipetakan menjadi A, dan A akan dipetakan menjadi F. Jika tidak ada sambungan huruf yang bersangkutan maka huruf tersebut tidak akan mengalami pemetaan. Setelah melewati *plugboard*, huruf akan dipetakan melalui 3 rotor. Tiap rotor mengandung satu pemetaan huruf tetapi berhubung rotor berputar untuk tiap penekanan tombol huruf sehingga pemetaan rotor berubah untuk tiap penekanan tombol. Setelah melewati 3 rotor selanjutnya diteruskan ke reflektor. Reflektor sangat mirip dengan rotor hanya saja reflektor tidak berputar sehingga pemetaan selalu sama. Keseluruhan proses enkripsi untuk satu huruf minimum mengandung 7 pemetaan (arus listrik mengalir melalui 3 Rotor sebanyak 2 kali) dan maksimum sebanyak 9 pemetaan (jika huruf tersambung ke *Plugboard*).

IV. Analisis Kombinatorik Pada Enigma

Secara matematis, proses enkripsi maupun dekripsi pada Enigma dapat dinyatakan sebagai berikut :

Misalkan :

γ : Permutasi pada *plugboard*

δ: Permutasi pada rotor kanan

μ: Permutasi pada rotor tengah

τ: Permutasi pada rotor kiri

η: Permutasi pada reflektor

E: Output hasil enkripsi/dekripsi

maka enkripsi / dekripsi pada Enigma merupakan permutasi panjang dari komponen-komponen Enigma yang melakukan pemetaan yaitu :

$$E = \gamma \cdot \delta \cdot \mu \cdot \tau \cdot \eta \cdot \tau^{-1} \cdot \mu^{-1} \cdot \delta^{-1} \cdot \gamma^{-1}$$

IV.a Plugboard

Plugboard memiliki 26 soket kontak yang mana tiap soket memiliki sebuah huruf. Operator dapat menggunakan 0 sampai 13 kabel, tidak semua koneksi huruf dimungkinkan. Tidak dapat dihubungkan dua huruf pada alphabet yang sama atau huruf tersebut ke dirinya sendiri. Jika tidak ada kabel yang digunakan maka hanya ada satu cara untuk pemetaannya, yaitu tidak ada perubahan pada pesan. Jika menggunakan satu kabel berarti ada dua huruf yang akan dihubungkan, maka ada 325 cara untuk pengaturan substitusi. Jika menggunakan dua kabel berarti ada empat huruf yang akan dihubungkan, maka ada 44.850 cara untuk pengaturan substitusi. Jika diberikan pilihan dari *p*-kabel pada plugboard yang akan dihubungkan ($0 \le p \le 13$) maka ada

$\binom{26}{2p}$ kombinasi substitusi pada soket yang dapat dipilih. Kemudian, banyaknya cara untuk memasangkan 2*p* huruf ke dalam *p* grup dimana grup-grup tersebut tidak dilabeli dan tidak memerhatikan urutan adalah (2*p* - 1)!!. Jadi jika dimiliki p-kabel yang akan dihubungkan ke 2p huruf, banyak kemungkinannya adalah

$$\binom{26}{2p}(2p-1)!!$$

Total banyaknya kombinasi substitusi yang mungkin dibuat oleh operator Enigma adalah

$$\sum_{p=0}^{13}\binom{26}{2p}(2p-1)!! = 5{,}32 \times 10^{14}$$

Karena mesin Enigma hanya menggunakan satu *plugboard*, maka pemecah sandi (cryptanalysists) harus bisa menebak dengan tepat banyak kabel yang digunakan. Dengan kata lain, harus ditebak substitusi *p* pasangan-pasangan huruf diantara 5.32 x 10^{14} kemungkinan pasangan-pasangan huruf yang berbeda.

IV.b Rotor-rotor

Rotor memiliki 26 input kontak yang dihubungkan dengan kawat ke 26 output kontak. Tiap rotor memiliki dua himpunan alphabet dengan aturan setiap huruf pada alphabet pertama dihubungkan dengan setiap huruf pada alphabet kedua, tetapi tidak pernah menghubungkan dua huruf dalam alphabet yang sama (Artinya tidak mungkin menghubungkan A dan B pada alphabet pertama ke C pada alphabet kedua, tetapi mungkin untuk menghubungkan A ke A). Pada mesin Enigma terdapat tiga rotor, banyaknya kemungkinan yang terjadi untuk tiga rotor ini adalah 26! $\cdot$(26! – 1)$\cdot$(26! –2). Pada Mesin Enigma M3, tersedia 8 rotor yang dapat dipilih, sehingga ada 8 x 7 x 6 = 336 kemungkinan untuk memilih 3 rotor dari 8 rotor. Setelah menentukan ketiga rotor yang akan digunakan, kemudian akan ditentukan posisi awal dari ketiga rotor tersebut. Operator dapat memutar rotor ke sebarang posisi awal yang diinginkan. Tiap rotor memiliki 26 kemungkinan untuk posisi awalnya, sehingga untuk ketiga rotor maka ada 26^3 = 17.576 kemungkinan untuk inisialisasi posisi awalnya. Elemen berikutnya adalah *notch. Notch* mengontrol ketika rotor berikutnya bergerak maju satu huruf. Banyaknya kemungkinan dari elemen ini adalah 26^2 = 676 kom. Berdasarkan perhitungan di atas, maka total banyaknya kemungkinan substitusi pada rotor-rotor adalah 2,61 x 10^{89}.

IV.c Reflektor

Analisis pada reflektor sama halnya pada plugboard yaitu memilih huruf yang akan dipasangkan kemudian memasangkan huruf

yang dipilih ke dalam grup (yang berisi dua elemen) . Banyaknya cara memilih 26 huruf dari 26 huruf ialah $\binom{26}{26}$ dan banyaknya cara untuk memasangkanhuruf tersebut menjadi sepasang-sepasang ialah (26 – 1)!!, sehingga banyaknya kemungkinan pada pengaturaan reflektor ialah

$$\binom{26}{26} \cdot (26-1)!! = 7.9x10^{12}$$

V. Kelemahan Enigma

Pada desain dasar Enigma terdapat beberapa kelemahan yang membantu pihak sekutu dapat memecahkan kode Enigma, yaitu

- **Sebuah huruf tidak mungkin dikodekan ke dirinya sendiri**

  Salah satu sifat utama dari desain Enigma adalah kenyataan bahwa sebuah huruf tidak dapat dikodekan ke dalam dirinya. Hal ini memungkinkan sekutu mempunyai peluang menebak huruf yang disubstitusi di dalam satu kata yang sama dalam dua pesan sandi yang berbeda apabila operator yang lalai tidak merubah pengaturan kunci pada kedua pesan tersebut. Sifat ini juga memperkecil banyak kemungkinan permutasi yang mungkin karena semua permutasi yg membawa satu huruf ke dirinya sendiri dikeluarkan dari perhitungan.

- **Loncatan umum dari rotor dalam kebanyakan mesin Enigma dan *notches* pada masing-masing rotor**

  Rotor kanan harus berputar penuh sebelum rotor disebelahnya berputar satu posisi. Akibatnya , 2 rotor hanya melangkah sekali setiap 26 karakter dan rotor 3 hampir tidak pernah bergerak. Namun pada Enigma M3, tiap rotor memiliki *notches* yang menyebabkan posisi *turnover* tiap rotor dapat diprediksi terutama pada 3 rotor tambahan (VI, VII, VIII) masing-masing dari rotor ini memiliki 2 *notches* yang diposisikan berlawanan. Hal ini membuat kode Enigma lebih mudah diprediksi.

- **Kewajiban menggunakan rotor tambahan**

  Jika operator dapat memilih 3 rotor dari 8 rotor yang tersedia, maka ada 336 kemungkinan susunan rotor-rotor. Namun dalam prakteknya, Angkatan Bersenjata Jerman (khususnya Angkatan Laut) diharuskan menggunakan minimal satu rotor tambahan setiap hari (VI, VII, VIII) dan bahwa rotor yang telah dipilih tidak dapat digunakan untuk dua hari berturu-turut.

- **Jumlah kabel yang tetap pada *Plugboard***

Plugboard memiliki 26 soket dimana tiap soket untuk tiap huruf dala alphabet. Dalam menghubungkan huruf pada *plugboard* digunakan sambungan dengan kabel. Secara teori, ada 0 sampai 13 jumlah kabel yang dapat digunakan. Tetapi pada prakteknya, operator diperintahkan hanya menggunakan tepat 10 kabel sepanjang waktu, yang mengakibatkan berkurangnya jumlah kemungkinan maksimum pada *plugboard*.

VI. Kesimpulan

a. Algoritma enkripsi dan dekripsi pada mesin Enigma adalah :

- ✓ Pilih 3 rotor dari 8 rotor yang tersedia lalu tentukan urutan dari 3 rotor yang dipilih.
- ✓ Mengatur posisi awal dari ketiga rotor sesuai kunci yang sudah ditentukan.
- ✓ Memilih reflektor yang akan digunakan.
- ✓ Mengatur pasangan huruf dalam *plugboard*.
- ✓ Input teks/pesan yang akan dienkripsi atau didekripsi.
- ✓ Catat huruf yang menyala pada panel lampu yang menyala setiap huruf ditekan.

b. Pada umumnya, mesin Enigma mengenkripsi dua huruf yang berbeda posisinya di dalam pesan dengan dua permutasi yang berbeda. Akibatnya, kripto dengan mesin Enigma adalah kripto Polialphabetik.

c. Kemungkinan banyaknya kombinasi substitusi pada komponen-komponen Enigma adalah:

- ✓ Plugboard : 532,985,208,200,576≈ 5.32 x 10^{14}
- ✓ Rotor : 261, 856, 342, 573, 250, 902, 230, 282, 229, 639, 117, 342, 628, 582, 862, 758, 366, 064, 488, 660, 115, 353, 068, 268, 501, 700, 968, 448, 000, 000 ≈ 2.61 x 10^{89}
- ✓ Reflektor : 7,905,853,580,625≈ 7.9 x 10^{12}

d. Kelemahan Enigma :

- ✓ Pesan dienkripsi sebanyak dua kali
- ✓ Pengaturan kunci tidak disamarkan dalam pesan yang ter-enkripsi yang dikirim
- ✓ Sebuah huruf tidak dapat dikodekan ke dirinya sendiri
- ✓ Loncatan umum dari rotor dalam kebanyakan mesin Enigma dan *notches* pada masing-masing rotor
- ✓ Kewajiban menggunakan rotor tambahan
- ✓ Penggunaan jumlah kabel yang tetap pada *plugboard*

VII. Daftar Pustaka

Cozzens, Midge, Steven Miller and Welsey Pegden. *The Mathematics Of Encryption: An Elementary Introduction*. 25 Oktober 2015. *https://web.williams.edu/Mathematics/sjmiller/public_html/tas2012CrytpoBenford/unithan*

douts/unit2_chap_Enigma_SchrockMiller.pdf

Dade, Louise. *How Enigma Machines Work*. 30 Desember 2015. *http://enigma.louisedade.co.uk/howitworks.html*

Miller,AR. 2008. *The Cryptographic Mathematics of Enigma*. *http://www.nsa.gov/publications/publi00004.cfm*